Tutorial 2:
WPA encryption cracking by dictionary attacks.

Mikhail Zolotukhin and Timo Hämäläinen

Department of Mathematical Information Technology, University of Jyväskylä

1 Introduction

This tutorial explains how to crack wireless networks encrypted with WPA by using dictionary attacks. For this tutorial, you are supposed to have two laptops with wireless interfaces (or one laptop and one smartphone) and wireless access point, e.g. WiFi router. One of the laptops will be used as a client and another one as an attacker. WiFi router must support WPA encryption. The remainder of this tutorial is organized as follows. Preliminary questions are listed in Section 2. Configuration of a wireless router and a client are presented in Section 3. Section 4 describes how to install and use BackTrack. The dictionary attack is demonstrated in Section 5. In Section 6, the dictionary attack is combined with brute forcing. Some simple assignments are listed in Section 7. Section 8 concludes the tutorial.

2 Preliminary questions

1. How does WPA tackle the WEP's IV weakness?
2. What are the weakest features of the WPA-PSK?
3. What are brute force and dictionary attacks?
4. Why the pure brute force technique is not effective for the WPA cracking?

3 Network configuration

3.1 WiFi router

1. Open the router settings web-page (usually it is 192.168.1.1).
2. Change the name of the wireless network name (SSID) to "dd-wrt" (you can choose another name, but, in this tutorial, we assume it is named this way).
3. Disable SSID broadcast. It will cause additional problem for the attacker to find the wireless network name.
4. Go to Wireless security settings and set the wireless security mode as WPA Personal and input the password. For the sake of demonstration, we assume that the password is "labra123".
5. Save and apply new settings.

3.2 Client

1. Create a wireless connection on the client. The way highly depends on the operation system of the client.
2. In this connection, input the name of your wireless network (in our case "dd-wrt“), set the security mode as WPA Personal and input your password (”labra123”).
3. Connect to the network and stay connected during the performing the attack.

4 BackTrack

BackTrack is a distribution based on the Debian GNU/Linux distribution aimed at digital forensics and penetration testing use. BackTrack provides users with easy access to a comprehensive and large collection of security-related tools ranging from port scanners to password crackers. You can download the latest version of BackTrack (BackTrack 5) from http://www.backtrack-linux.org/downloads/. You can boot BackTrack as a USB thumb drive with the help of LinuxLive USB Creator. There are several tips for the BackTrack installation and starting:

1. When loading BackTrack from USb you can get the following error:

   ```
   Could not find kernel image:vesamenu.c32
   ```

   To solve this, hit Tab (you will see possible variants of booting) and type `DEFAULT`.
2. Once BackTrack has been installed you can login as a root by using login ”root” and password ”toor”.
3. After you have logged in, type `startx` in the command window in order to open BackTrack graphical interface.

5 Dictionary Attack

1. Open a terminal and type

   ```
   airmon-ng
   ```

   It will show you all wireless interfaces of your system, e.g. wlan0, wlan1, etc and their statuses. You should choose one of the interfaces which will be used for the attack. In this tutorial, the interface wlan1 is used.
2. Type

   ```
   rfkill list
   ```

   and check that wireless LAN is not blocked (in my case, it was hard blocked by default). If yes, unblock it by typing:

   ```
   rfkill unblock wifi
   ```

   Otherwise, just skip this step.
3. Stop the wlan1 interface:

   ```
   airmon-ng stop wlan1
   ```

   and disable it:

   ```
   ifconfig wlan1 down
   ```

4. Spoof the mac address of the attacker laptop:

   ```
   macchanger --mac 00:11:22:33:44:55 wlan1
   ```

5. Restart the interface wlan1 with new mac:

   ```
   airmon-ng start wlan1
   ```

   It will put your card into monitor mode. Monitor mode is mode whereby your card can listen to every packet in the air. Normally your card will only hear packets addressed to you. In addition, monitor mode allows you to inject packets. You will see that monitor mode enabled on mon0 (the number can be different).

6. Using the interface mon0 start monitoring available wireless networks by typing:

   ```
   airodump-ng mon0
   ```

   You will see a list of available wireless networks. Find the network corresponding to the WiFi router you have configured:
   - Its BSSID must be equal to the MAC address of the router
   - Encryption mode is WPA
   - ESSID is hidden (in our case it's named ¡length: 6¿, because wireless network name ”dd-wrt” has 6 symbols).

   Please make sure that you pick the network corresponding to your router, but not the one belonging to your neighbour. After you have found the target network, check what channel it uses. It is needed for the next step. Hit CTRL+C to cancel the running airodump.
7. Configure airodump-ng to watch the target network, capture the unique data holding the password and put it into a file:

   ```
   airodump-ng -c (channel) -w (filename) --bssid (BSSID) (interface)
   ```

   For example, in my case it looks as follows:

   ```
   airodump-ng -c 6 -w /root/Desktop/hackedwpa --bssid 58:6D:8F:6B:28:81 mon0
   ```

   It will start monitor the target network and put all the data into file “hackedwpa“ located in the directory ”/root/Desktop/“. As the output you will see two parts. The first one contains information about your wireless network: BSSID, data, channel, encryption, etc. The second part contains information about clients connected to this network. In particular, one can see the client MAC address in the column STATION, which is needed for the next step of the attack. If the part corresponding to the clients is empty, try to open several webpages on the client machine which is connected to the target wireless network.
8. To get the hidden ESSID we have to de-authenticate the client and get the ESSID during client's re-authentication. For this purpose, open the second terminal on the attacker machine and type:

   ```
   aireplay-ng -0 1 -a (BSSID) -c (station) (interface)
   ```

   For example, in my case it looks as follows:

   ```
   aireplay-ng -0 1 -a 58:6D:8F:6B:28:81 -c C4:17:FE:F8:BE:C7 mon0
   ```

9. Switch back to the first terminal window that still has airodump-ng running. You can see the name of the target wireless network (”dd-wrt”) has appeared. In addition to that, in the top right corner of terminal you are supposed to see the following message:

   ```
   WPA handshake: (BSSID)
   ```

   that means that an authentication handshake has been captured (if this message did not appear, try to repeat steps 4 – 8 accurately). Hit CTRL+C to cancel the running airodump.
10. Download the wordlist from http://users.jyu.fi/ mizolotu/download.php?file=files/password.lst. It is not compulsory to use this wordlist. There are plenty of wordlists in the Internet and you are encouraged to use some of them. Look within the list and if your password is not presented in the list, add it somewhere in the middle for the sake of demonstration. Name the wordlist you are planning to use as “password.lst“ and put it to the directory ”/root/Desktop/“.
11. Start a dictionary attack against a WPA key as follows:

    ```
    aircrack-ng -e (ESSID) -w (dictionary_file) (capture_file-01.cap)
    ```

    that in our case looks like this:

    ```
    aircrack-ng -e dd-wrt -w /root/Desktop/password.lst
    /root/Desktop/hackedwpa-01.cap
    ```

    Wait for a while and the password will be found.

6 Extention of the dictionary attack

The obvious limitation of the technique described in the previous section is the existence of the key within the dictionary file used for the attack. To extend the list of possible keys, we can use wordlist mangling rules to generate permutations and common password additions from a simple dictionary file.

1. Let us assume that our password ”labra123” (or the password you used) is not presented in the wordlist “password.lst”, but the word “labra” is there. Open the file “password.lst” and exchange ”labra123” with “labra“ in the list. Thus, the standard dictionary attack with wordlist ”password.lst” will not be effective.
2. To create rules for generating new words from the password list the application John The Ripper is used. John comes with a built-in set of rules that is fairly limited, but uses a well documented ”regex-esque” syntax that allows you to define your own rules. Let us add new rules according to which two digits will be added to the end of each word in the password list. Open the file ”john.conf” in the directory ”/pentest/passwords/john” (directory name can be different in different versions of BackTrack):

   ```
   gedit /pentest/passwords/john/john.conf
   ```

   Find [List.Rules:Wordlist] section. It corresponds to the rules which will be applied to the wordlist. As you can see it already contains several rules. Add the following line to the end of this section:

   ```
   $[0-9]$[0-9]$[0-9]
   ```

   It will add any combination of two digits to the end of each word in the wordlist. Save changes.
3. We can apply these rules and find the password with the help of Aircrack. However, to demonstrate another BackTrack application, we use CowPatty. It automates the dictionary attack for WPA-PSK. The program is started using a command-line interface, specifying a word-list that contains the passphrase, a dump file that contains the WPA handshake, and the ESSID of the network. Change directory to “/pentest/passwords/john”.

   ```
   cd /pentest/passwords/john
   ```

   and type the following command in the terminal:

   ```
   ./john --wordlist=(password_list) --rules
   --stdout | cowpatty -s (ESSID) -f - -r (capture_file-01.cap)
   ```

   which in our case looks as follows:

   ```
   ./john --wordlist=/root/Desktop/password.lst --rules --stdout |
   cowpatty -s dd-wrt -f - -r /root/Desktop/hackedwpa-01.cap
   ```

   Wait a few minutes and the password “labra123“ will be found.

7 Assignment

1. Answer preliminary questions and shortly explain the results obtained in the tutorial.
2. Taking into account the information given in this tutorial, propose simple rules how to choose a secure password for the WPA-PSK encryption mode.
3. What are other simple countermeasures that you can take to secure the wireless network with WPA-PSK?
4. Write general comments about the tutorial: what was interesting, difficult, etc.

Write a report (in English) where include answers for assignments above and send it to **mizolotu@jyu.fi**.

8 Conclusion

Despite the fact, that pure brute force is not effective for the cracking of the WPA encryption mode, attackers are able to crack it with the help of different dictionary attacks. In this tutorial, this type of the attack is demonstrated by using different BackTrack applications: Aircrack, CowPatty and John The Ripper.